



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-------------------------|---------------------|------------------|
| 10/735,388 | 12/12/2003 | David Carroll Challener | RPS920020048US1 | 1698 |

63203 7590 08/08/2006

ROGITZ & ASSOCIATES
750 B STREET
SUITE 3120
SAN DIEGO, CA 92101

EXAMINER

BANKS, CORBANN

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2192

DATE MAILED: 08/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/735,388

Applicant(s)

CHALLENGER ET AL.

Examiner

Corbann A. Banks

Art Unit

2192

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 December 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>12/12/2003</u> <i>5/10/4</i> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Informalities

Figures 1 and 2 are objected to because they were not legibly constructed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim(s) 1 – 6, 8 – 12, 14 – 18, and 20 – 23 are rejected under 35

U.S.C. 102(a) as being anticipated by Wheeler et al. (US PGPub # 2003/0097569).

Claim(s) 1 – 6, 8 – 12, 14 – 18, and 20 – 23 are also rejected under 35 U.S.C. 102(e (1)) as being anticipated by the patent of Wheeler et al. (US Patent # 6,915,430 B2).

Here, Wheeler clearly shows a method / computing device / service / computing facility that provides an endorsement key pair to a security module associated with a customer computing device (see column 6, lines 30 - 55), storing data representative of the public key in a storage external to the customer device (see column 6, lines 30 - 55), at a

Art Unit: 2192

subsequent time, receiving at a comparison agent operatively connected to the storage, certificate request data from the customer device (see columns 1, 6, and 17 lines 44 – 67, 17 – 18, and 24 – 52), the certificate request data including at least one of: the public key, and a hash of the public key with a temporary secret (see columns 1, 6, and 7 lines 44 – 67, 1 – 29, and 8 – 18), determining whether at least a portion of the certificate request data transmitted to the comparison agent matches the data representative of the public key stored in the storage (see column 6, lines 1 – 11), and if so: generating an endorsement certificate at least in part using the public key (see column 7, lines 8 – 18), and providing the endorsement certificate to the customer device (see columns 7 and 8, lines 8 – 18 and 4 – 17); wherein the receiving act is associated with a request from the customer device for the endorsement certificate (see columns 1, 6, and 17 lines 44 – 67, 17 – 18, and 24 – 52); further comprising transferring the customer device to a customer after the storing act (see column 7, lines 44 – 58); wherein the security module is a trusted platform module (TPM) (see column 15, lines 4 – 8); wherein the storage / source of endorsement certificates, and the comparison agent are not associated with a vendor of the customer device (see column 16, lines 28 – 30); further comprising signing the endorsement certificate with a signing key (see column 7, lines 13 – 15 and 25 – 28) before transmitting the endorsement certificate to the customer device.

Claim(s) 1 – 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Trusted Computing Platform Alliance (Main Specification v 1.1b, February 2002, herein after TCG). Here, TCG clearly shows a method / computing device / service / computing facility that provides an endorsement key pair to a security module associated with a customer computing device (see page 262, section 9.2), storing data representative of the public key in a storage external to the customer device (see page 145, section 7.1), at a subsequent time, receiving at a comparison agent operatively connected to the storage, certificate request data from the customer device (see page 275, "TCPA_IDENTITY_REQ"), the certificate request data including at least one of: the public key, and a hash of the public key with a temporary secret (see page 306, sections 10.4.6 – 10.4.7), determining whether at least a portion of the certificate request data transmitted to the comparison agent matches the data representative of the public key stored in the storage (see page 303, section 10.3), and if so: generating an endorsement certificate at least in part using the public key (see pages 283 - 285, section 9.5.1), and providing the endorsement certificate to the customer device (see page 283, section 9.5.1); wherein the receiving act is associated with a request from the customer device for the endorsement certificate (see page 275, step 7 (receiving "Return" act naturally follows "request"))); further comprising transferring the customer device to a customer after the storing act (see page 283, paragraph immediately above "Overview" heading); wherein the security module is a trusted platform module (TPM) (see page 8, section 2.5); wherein the storage / source of endorsement certificates, and the comparison agent are not associated with a vendor of the customer device (see

page 145, section 7); further comprising signing the endorsement certificate with a signing key (see pages 7 and 283, sections 2.4 and 9.5.1) before transmitting the endorsement certificate to the customer device; wherein the temporary secret is erased from the security module (within the customer computing device) after the certificate request data (i.e. data representative of the public key) has been sent to the comparison agent / source (i.e. facility - see page 14, section 3.1, last paragraph).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim(s) 7, 13, 19, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al. (US Patent # 6,915,430 B2), in further view of Trusted Computing Platform Alliance (Main Specification v 1.1b, February 2002, herein after TCG). The reference of Wheeler have been discussed above. Wheeler teaches receiving at a comparison agent operatively connected to the storage, certificate request data from the customer device, the certificate request data including at least one of: the public key, and a hash of the public key with a temporary secret (see columns 1, 6, and 7 lines 44 – 67, 1 – 29, and 8 - 18). However, Wheeler does not teach erasing the temporary secret from the security module after the certificate request data has been sent to the comparison agent.

On the other hand, TCG does teach how data accessed by the Subsystem (i.e. the temporary secret from the security module) could be erased after conversion (using a protected capability) into another data structure (i.e. the endorsement certificate). (See page 14, section 3.1, last paragraph.)

Thus, it would have been obvious to one skilled in the art to have included such a step in the invention taught by Wheeler above, to protect the temporary secret from being inadvertently transmitted or otherwise compromised.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Corbann A. Banks whose telephone number is (571) 270-1021. The examiner can normally be reached on Monday - Thursday from 8:00am to 4:00pm. The examiner can also be reached on alternate Fridays during the same hours.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David L. Robertson, can be reached at (571) 272- 4186 during the same days and hours. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Application/Control Number: 10/735,388

Page 7

Art Unit: 2192

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A handwritten signature in black ink, consisting of the letters 'C' and 'B' followed by a period, written in a cursive style.

Corbann Banks

July 18, 2006